From Cybercrime to Digital Crime: Assessing the Effectiveness of Islamic Law Enforcement Against Cracking in Makassar City

Riswandi Riswandi [1], Muhammad Kamal Hidjaz[2], Yuli Adha Hamza[3]

[1,2,3] Faculty of Law, Universitas Muslim Indonesia, Indonesia

Surel Koresponden: Wandir192@gmail.com

Abstrak: Perkembangan teknologi informasi telah melahirkan bentuk kejahatan baru yang dikenal sebagai cybercrime, salah satunya adalah cracking, yaitu tindakan pembobolan sistem keamanan komputer secara ilegal yang berdampak pada kerugian ekonomi, pelanggaran privasi, dan gangguan terhadap stabilitas sistem elektronik. Penelitian ini bertujuan untuk menganalisis efektivitas penegakan hukum terhadap tindak pidana cracking di Kota Makassar serta mengkaji fenomena tersebut dalam perspektif hukum Islam sebagai jarimah digital. Metode penelitian yang digunakan adalah pendekatan yuridis empiris integratif, dengan menggabungkan analisis hukum positif dan kajian normatif hukum Islam. Data diperoleh melalui wawancara dengan aparat penegak hukum, observasi lapangan, serta studi dokumentasi terhadap peraturan perundang-undangan dan literatur ilmiah. Hasil penelitian menunjukkan bahwa penegakan hukum terhadap tindak pidana cracking di wilayah hukum Kepolisian Daerah Sulawesi Selatan telah berjalan, namun belum optimal. Hal ini disebabkan oleh berbagai kendala, antara lain keterbatasan sumber daya manusia yang memiliki kompetensi digital forensik, minimnya sarana dan prasarana teknologi, serta kompleksitas pembuktian dalam kejahatan siber. Selain itu, rendahnya kesadaran hukum masyarakat turut menjadi faktor penghambat dalam pengungkapan kasus. Dalam perspektif hukum Islam, cracking dapat dikategorikan sebagai jarimah ta'zir karena tidak diatur secara eksplisit dalam nash, namun bertentangan dengan prinsip maqashid al-shariah, khususnya dalam perlindungan harta (hifz al-mal) dan kehormatan (hifz al-'irdh). Hukum Islam menawarkan pendekatan yang komprehensif melalui mekanisme sanksi yang fleksibel, serta menekankan aspek preventif, edukatif, dan moral dalam penanggulangan kejahatan. Oleh karena itu, efektivitas penegakan hukum terhadap cracking memerlukan pendekatan integratif antara hukum positif dan nilai-nilai hukum Islam guna mewujudkan sistem hukum yang adaptif, berkeadilan, dan berorientasi pada kemaslahatan di era digital.

Kata Kunci: Cracking, Kejahatan Siber, Penegakan Hukum, Hukum Islam, Jarimah Ta'zir

***Abstract**: The rapid development of information technology has given rise to new forms of crime known as cybercrime, one of which is cracking, defined as the illegal act of breaching computer security systems that results in economic losses, violations of privacy, and disruption of electronic system stability. This study aims to analyze the effectiveness of law enforcement against cracking offenses in Makassar City and to examine the phenomenon from the perspective of Islamic law as a form of digital jarimah. The research employs an integrative empirical juridical approach, combining positive legal analysis with normative Islamic legal perspectives. Data were collected through interviews with law enforcement officers, field observations, and documentation studies*

of statutory regulations and relevant academic literature. The results indicate that law enforcement against cracking offenses within the jurisdiction of the South Sulawesi Regional Police has been implemented, yet remains suboptimal. This condition is influenced by several constraints, including the limited number of personnel with digital forensic expertise, inadequate technological infrastructure, and the complexity of evidentiary processes in cybercrime cases. Additionally, low public legal awareness contributes to the underreporting and difficulty in uncovering such crimes. From the perspective of Islamic law, cracking can be classified as a ta'zir jarimah, as it is not explicitly regulated in the primary sources (nash), yet it contradicts the principles of maqashid al-shariah, particularly in the protection of property (hifz al-mal) and honor (hifz al-'irdh). Islamic law offers a comprehensive approach through flexible sanction mechanisms, while also emphasizing preventive, educational, and moral dimensions in addressing crime. Therefore, the effectiveness of law enforcement against cracking requires an integrative approach between positive law and Islamic legal values in order to establish a legal system that is adaptive, just, and oriented toward public welfare in the digital era.

Keywords: *Cracking, Cybercrime, Law Enforcement, Islamic Law, Ta'zir Crimes*

A. INTRODUCTION

The development of information and communication technology in the digital era has brought about significant changes in various aspects of human life. Technology no longer functions merely as a communication tool, but has become a vital part of economic activities, education, government, public services, trade, and even social relations. Through digitalization, various activities can be carried out more quickly, practically, and efficiently. People can conduct financial transactions, access information, use public services, and interact without being limited by space and time. However, these technological advances do not always have a positive impact. Despite their significant benefits, technological developments also open up opportunities for the emergence of new, more complex, modern, and difficult-to-detect forms of crime.[1] One form of crime born from these technological developments is cybercrime. Cybercrime is a form of crime committed using computers, internet networks, electronic systems, or digital devices as both a means and a target. Unlike conventional crimes, which are generally committed directly and whose perpetrators are easily identified, cybercrime is more complex because it can be carried out covertly, anonymously, across regions, and even across countries. Cybercriminals can attack electronic systems without having to be in the same location as the victim. This situation demonstrates that technological progress has two opposing sides. On the one hand, technology is an instrument of progress and makes human life easier, but on the other, it can also be exploited as a means to commit irregularities, violations of the law, and crimes.[2]

One increasingly widespread form of cybercrime is cracking. Cracking is the act of illegally breaking into or destroying the security of a computer, network, or electronic system to gain unauthorized access. This action is usually carried out with the aim of stealing data, altering information, damaging the system, gaining economic advantage, or disrupting the activities of certain parties. Cracking differs from legitimate security testing activities because it is carried out without authorization and is against the law. In practice, cracking can attack various objects, such as personal accounts, banking systems, company databases, government websites, and public service systems. Therefore, cracking cannot be viewed as a simple act, but rather as a modern form of crime with a broad impact on digital security. The impact of cracking is not limited to material losses but also involves broader non-material losses. Materially, victims can experience financial loss, system damage, data leaks, and losses due to disruption of business activities or services.[3] Meanwhile, non-materially, cracking can lead to a loss of security, damage to an institution's reputation, diminished public trust in electronic systems, and violations of individual privacy rights. In today's digital world, data holds crucial value because it concerns identity, financial information, personal documents, and institutional interests. If this data is illegally accessed or misused, the resulting losses can have significant consequences for the victim. Therefore, cracking needs to be understood as a serious crime that threatens security, order, and trust in the digital space.[4]

Within the context of positive law in Indonesia, cracking has received attention through legal regulations in the field of information and electronic transactions. Law Number 11 of 2008 concerning Information and Electronic Transactions, as amended by Law Number 19 of 2016, provides the legal basis for prohibiting illegal access, interference with electronic systems, unauthorized interception, and other acts that damage or disrupt electronic systems. These provisions demonstrate the state's efforts to provide legal protection for the security of electronic systems and digital data.[5] This regulation is crucial because public activities are increasingly dependent on electronic systems, so any form of violation of digital security can have serious legal consequences.[6] Despite existing legal regulations, law enforcement against cybercracking crimes still faces various challenges. The anonymous nature of cybercrime makes it often difficult to identify perpetrators. Furthermore, these crimes can be committed from a different location than the victim, raising jurisdictional issues. In the process of establishing evidence, law enforcement requires not only conventional evidence but also digital evidence, which must be properly obtained, secured, and analyzed. Digital evidence is volatile and easily deleted, and requires specialized expertise during the examination process. This requires digital forensic skills, adequate technological tools, and strong coordination between law enforcement officials, electronic service providers, and other relevant parties.[7]

In Makassar City, information technology development has also experienced significant growth. As one of the major cities and a center of economic growth in Eastern Indonesia, Makassar experiences increasing digital activity in the government, trade, education, banking, and public services sectors. This increased use of technology undoubtedly has a positive impact on service effectiveness and digital economic growth. However, on the other hand, the public's increasing dependence on electronic systems also opens up opportunities for cybercrime,

including cybercracking. The more systems used by the public and institutions, the greater the potential for those systems to become targets for attacks by irresponsible parties. The police, particularly units handling cybercrime, play a crucial role in preventing and prosecuting cybercrime. Law enforcement efforts are carried out through investigations, inquiries, digital evidence collection, tracking down perpetrators, and bringing cases to justice. However, in practice, these efforts are not always straightforward. The limited human resources with specialized expertise in information technology and digital forensics are major obstacles. Furthermore, limited technological infrastructure, increasingly sophisticated modus operandi of perpetrators, and low public awareness of data security also hamper the effectiveness of law enforcement. This situation demonstrates that handling cybercrime cannot simply rely on legal regulations; it also requires technical and institutional readiness and public education.[8]

Beyond its legal perspective, cybercrime is also important to examine from an Islamic legal perspective. Islamic law not only regulates the relationship between humans and God but also regulates relationships between humans, including the protection of rights, property, security, and honor. From an Islamic legal perspective, cracking can be categorized as a jarimah (criminal offense) or criminal act because it contains elements of an act that harms others, is carried out without authorization, and violates the principles of justice and public interest. Although cracking is not explicitly mentioned in the texts, as it is a form of modern crime, the substance of the act can be linked to the prohibition of taking another's rights unlawfully, destroying property, violating trusts, and causing harm to others. Cracking, under Islamic law, can be categorized as jarimah ta'zir (criminal offense), a type of crime whose form and sanctions are not specifically specified in the Quran and Hadith, but are delegated to the authority of ulil amri (the people in authority) or the government for the sake of maintaining order and the public interest. The ta'zir category is relevant because Islamic law is dynamic in responding to developments, including crimes arising from technological advancements. Through the concept of ta'zir, the state or authorized authorities can impose sanctions on crackers according to the level of culpability, the impact of the harm, and the importance of protecting society. Thus, Islamic law provides room for adaptive responses to digital crime, as long as it remains based on the principles of justice, prevention of harm, and protection of human rights.

Within the framework of the maqasid al-Shariah (Islamic law), cracking contradicts the objectives of Islamic law, particularly in protecting property (hifz al-mal), protecting life and security (hifz al-nafs), and protecting honor and privacy. Digital data, electronic accounts, information systems, and virtual assets today have a value comparable to property or interests that must be protected. When someone breaks into an electronic system without permission, steals data, or damages the system, such actions essentially violate the property rights and security of others. Furthermore, cracking also violates the principle of la dharar wa la dhirar, which prohibits actions that cause harm or loss to others. Therefore, Islamic law views cracking not only as a technical violation but also as a moral and social violation.

The Islamic legal approach to the crime of cracking focuses not only on imposing sanctions but also on prevention and fostering moral awareness. Islam emphasizes the importance of trustworthiness, honesty, responsibility, and the prohibition against misusing one's abilities to

harm others. In the digital context, technological mastery should be used for good, security, and welfare, not to damage systems or take away the rights of others. Therefore, an Islamic legal approach can provide added value in combating cybercrime, as it not only regulates the external aspects of actions and sanctions, but also addresses the internal aspects of ethical awareness and moral accountability before Allah SWT. Based on this description, this study seeks to examine the transformation of the crime of cracking from a positive legal perspective toward the construction of digital crimes within Islamic law. This study is important because technological developments have given rise to new forms of crime that require a legal approach that is not only normative but also adaptive and responsive to social realities. This research is also relevant in the context of Makassar City, given that the increasing use of information technology has the potential to be followed by an increased threat of cybercrime. By combining positive legal and Islamic legal approaches, this study is expected to provide a more comprehensive understanding of how cracking can be handled, from the perspective of law enforcement, victim protection, and crime prevention.

The main focus of this research is to assess the effectiveness of law enforcement against cracking practices in Makassar City and to analyze how an Islamic legal approach can be used to respond to this crime. The research questions include: how to enforce the law against cracking crimes in Makassar City, and how effective the Islamic legal approach is in responding to and overcoming cracking crimes. This research is expected to provide theoretical contributions to the development of contemporary Islamic criminal law, particularly in responding to the ever-evolving dynamics of cybercrime. Furthermore, this research is also expected to provide practical recommendations for law enforcement officials, the government, and the public in building a more integrative, adaptive, and effective law enforcement system oriented toward substantive justice and the public good.

B. METHOD

This research uses an integrative empirical juridical approach, which combines analysis of positive law with normative studies of Islamic law in understanding the phenomenon of cybercrime, particularly cracking as a form of digital crime.[9] This approach was chosen to obtain a comprehensive picture of how the law is enforced in practice and how Islamic legal values can be used as an analytical framework in assessing the effectiveness of such law enforcement. Empirically, this research focuses on the practice of law enforcement against the crime of cracking by the police, while normatively, this research examines the concept of ta'zir crime, the principles of maqashid al-shariah (especially hifz al-mal and privacy protection), and relevant fiqh rules in responding to technology-based crimes. Thus, this research not only assesses the effectiveness of law enforcement from a procedural aspect, but also from the perspective of substantive justice in Islamic law. The research location is set in Makassar City, with the main locus being the South Sulawesi Regional Police, specifically the unit that handles cybercrime (cybercrime unit).

C. DISCUSSION

1. Law Enforcement of Criminal Acts of Computer Security Data System Hacking (Cracking) in Makassar City.

Cracking is the act of breaking into a computer system, hereinafter referred to as a PC, with the goal of gaining access. Conversely, those who practice cracking are called crackers. Cracking involves breaking into paid applications so that registration can be carried out without requiring a formal license purchase from the application developer. This is done with the intention of meeting certain requirements for the paid application to function optimally. Registration is generally required, or at least, the registration number is not entered. Cracking an application involves modifying software to remove or disable unwanted features. Cracking an application generally involves protection against "application manipulation, trial or demo versions, serial numbers, hardware keys, verification errors, CD checks, or problematic software such as screen capture and adware." The distribution and use of cracked copies is illegal in many countries. There have been lawsuits against forty-four cracked software programs, so cracking is clearly illegal. Crackers generally attempt to access a PC system without authorization. These individuals are generally malicious or unscrupulous, the opposite of "hackers," and typically earn money by infiltrating systems. Crackers, or tools used to crack applications for most antivirus programs, are often mistaken for viruses or Trojans. A Trojan horse is a program that appears to perform its intended function but, unknowingly, also performs other, generally harmful, activities. Trojan horses are generally used to create a "backdoor" that attackers can exploit to gain access to a PC system, making it easier to carry out attacks. They are also commonly used as spyware that can detect a victim's PC activity. A PC virus is a program capable of self-replicating itself, eventually spreading and inserting itself into executable programs and other types of files. The philosophy of a virus on a PC is the same as that of a virus in real life. Viruses are categorized as disruptive, malicious programs, or malware.[10]

As explained earlier, if we remain guided by the principle of legality, it will be difficult to apply the regulations contained in the Criminal Code to cracking cases. In this regard, an interpretation of the law is needed so that an act that is not regulated in the law is not simply set aside because there are no regulations or provisions. The courage of the judge to interpret the law is a form of anticipation of "CC", especially regarding Cracking. The application of the Criminal Code to the crime of cracking requires sorting out which acts have almost the same substance as the formulation of ordinary crimes in the Criminal Code. In the Criminal Code there are rules that regulate the destruction or destruction, namely in Article 406 paragraph (1) of the Criminal Code, which is formulated as follows: "Whoever intentionally and unlawfully destroys, damages, makes unusable or removes something, whether in whole or in part, belonging to another person, is threatened with imprisonment of two years and eight months or a maximum fine of four thousand five hundred rupiah." On April 23, 2008, the ITE Law was enacted, this law is not a special criminal law, besides that it is also related to the regulation of ITE management for development purposes, but this law also protects from negative influences by the benefits of increasing ITE technology. This applies specifically to criminal law enforcement, specifically regarding criminal acts that violate the legal needs of individuals, citizens, and the state's legal needs in utilizing advanced information and communication technology (ITE) technology, commonly referred to as

"cracking." In terms of law enforcement, particularly in the area of cybercrime, these crimes span a vast range without recognizing national territorial borders due to their "transnational" nature. This borderless form of crime requires direct state jurisdiction, as it is far beyond the reach of any other country. Without proper interstate contact when enforcing and enforcing the law, these transnational crimes can result in individual problems related to power.[11]

"Breaking embodies the act or activity of breaking into something. "Breaking" means "breaking into, disrupting, breaking into, disrupting with cruelty, or breaking into with force." Criminal responsibility essentially implies reciprocity for the perpetrator's actions for the crime committed. Therefore, criminal responsibility contains both object and subject elements. This means that, in fact, the perpetrator of the crime has committed a criminal offense, and the individual who committed the crime is culpable for the offense and can be punished. According to Mr. Mokhamad Ngajib, Head of the Cyber Crime Unit at the Makassar City Police, the process of investigating cybercrime is generally similar to handling other conventional crimes, except for several specificities, such as the implementation of the device by a special unit, the cyber unit. Furthermore, handling cybercrime investigations is also more complex because it requires comprehensive coordination with other agencies related to the crime. The series of investigator activities in conducting an investigation are inquiry, prosecution, examination, and completion of case files.

Therefore, it can be concluded that at this stage, investigators must be able to prove the crime occurred, as well as the manner and cause of the crime, in order to determine the form of the police report to be prepared. Information is usually obtained from the NCB/Interpol, which receives a notification letter or report from another country, which is then forwarded to the designated cybercrime unit. In investigating cracking cases, which involve methods such as carding, the methods used are almost the same as those used in drug crime investigations, particularly undercover and controlled delivery.[12]

From one of the residents who became a victim of a computer system hacking crime named M Radit Al Hafids as CV Labirin House said: I have experienced a data breach once, my employee data was used by an irresponsible person for Pinjol (online loans) I also panicked because there was a report from my employee that there was an online loan collection while my employee had never borrowed from the loan application, after we reported this incident to the Cyber Section of the Makassar Police, we were told that the data from the Open Recruitment that we distributed in the form of a Google form had been hacked and caused more than 100 registrants' personal data to be hacked. After the victim filed a complaint with the Makassar City Police Cyber Unit, the police encountered obstacles in handling the case. According to Cracking, Mr. Mokhamad Ngajib, Head of the Cyber Crime Unit at the Makassar City Police, stated: Cybercrime cases often encounter obstacles, especially in arresting suspects and confiscating evidence. When arresting suspects, it is often impossible to definitively identify the perpetrator because they operate on computers, which can be accessed from anywhere without anyone knowing, so there are no direct witnesses. The most we can do is find the IP address of the perpetrator and the computer used. This becomes even more difficult when using an internet cafe, as it is currently rare for internet cafes to register their users, making it impossible to determine who was using the computer at the time of the crime. Confiscation of evidence often encounters problems because the reporter is often very slow in reporting the crime.

Criminal acts are often referred to as crimes or criminal acts in some literature. Crimes that can only occur through the use of a computer network are known as cybercrimes, or simply put, crimes that use computers as the primary medium. Cybercrime specializes in identifying perpetrators and committing crimes, unlike crimes under the Criminal Code, where the process of uncovering and proving the crime and the perpetrators is guided by the provisions of the Criminal Code. Based on these actions, the perpetrator can be subject to criminal penalties. According to the principles of criminal law, an act cannot be punished unless there is a prior legal force, also known as Nullum delictum nulla poena sine praevia lege poenali. Therefore, a person can only be held criminally responsible for an act specifically prohibited by law.

The Indonesian government has attempted to address these hacking cases by establishing a legal framework covering these matters, including Law No. 36 of 1999 concerning Telecommunications, Law No. 19 of 2002 concerning Copyright, and Law No. 15 of 2003 concerning the Eradication of Terrorism, Law No. 11 of 2008 concerning Electronic Information and Transactions, and Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008. These laws criminalize forms of cybercrime, along with the threat of criminal sanctions for individuals who violate them. 11 However, there are still many hackers out there who continue to carry out their actions to hack both personal accounts and government websites. This can occur because cybercrime is difficult to identify with certainty, considering that it is carried out in the electronic environment and cyberspace. The Indonesian criminal law system explains that its legal provisions only apply to citizens and their own jurisdiction, also known as the territorial principle and the active personal/national principle. A factor that often becomes an obstacle in law enforcement in combating transnational crime, including cybercrime, is the determination of jurisdiction. The obstacles in determining jurisdiction regarding cybercrime can be overcome by the provisions in Article 2 of the Law on Information and Electronic Transactions which can be applied to anyone who commits a legal act stipulated in this regulation, both within and outside of Indonesian jurisdiction, has legal consequences within and/or outside of Indonesian jurisdiction and is detrimental to Indonesia's interests. With this provision, it is hoped that it can resolve the problem that if the perpetrator comes from outside of Indonesian jurisdiction, he can still be subject to criminal penalties.

Article 30 of the Law on Information and Electronic Transactions explains provisions that specifically regulate the definition of the crime of hacking, which interprets that anyone who tries to access another person's electronic system or computer intentionally and unlawfully with the aim of obtaining electronic information or documents. Then further explained in Article 46 of the ITE Law regarding the criminal threats that can be imposed on hackers. Article 46 paragraph (1) states that anyone who meets the criteria in Article 30 paragraph 1 can be sentenced to a maximum of 6 years in prison and/or a maximum fine of IDR 600,000,000.00. Then in Article 46 paragraph (2) states that anyone who meets the criteria in Article 30 paragraph 2 can be sentenced to a maximum of 7 years in prison and/or a maximum fine of IDR 700,000,000.00. Furthermore, Article 46 paragraph (3) states that anyone who meets the criteria in Article 30 paragraph 3 can be sentenced to a maximum of 8 years in prison and/or a maximum fine of IDR 800,000,000.00. There are increased penalties for hacking crimes, in addition to the criminal threats outlined in Article 46 of the

ITE Law. The increased penalties in this case are differentiated according to the subject and object. Based on the object, as stated in Article 52 paragraph (2) of the ITE Law, which increases the imposition of penalties if the hacked electronic system belongs to the government or a public service system. This increased penalty is the principal penalty plus one-third. Article 52 paragraph (3) of the ITE Law also explains that if the hacked website belongs to a state that has a direct relationship with the security and stability of the state, then increased criminal sanctions will be imposed. The increased penalty in Article 52 paragraph (3) is the principal penalty for each article plus two-thirds. Then, based on the subject, as stated in Article 52 paragraph (4) of the ITE Law, if the hacker is a corporation or company, the increased criminal penalty will be applied, namely the principal penalty plus two-thirds. In order to achieve criminal law enforcement, law enforcers should also use Article 52 paragraph (3) of the ITE Law as "... aimed at Computers and/or Electronic Systems as well as Electronic Information and/or Electronic Documents belonging to the Government and strategic bodies... are threatened with a maximum penalty of the principal penalty of each Article plus two-thirds" to be applied to crackers of government-owned electronic systems as an effort to realize benefits and legal certainty. The government-owned electronic systems referred to are in defense institutions, central banks, banking, finance, international institutions, aviation authorities. In addition, to see the meaning of "strategic bodies including and not limited to..." can also use Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. Institutions that must be protected because they contain strategic electronic data as per Article 99 paragraph (2) include; the government administration sector, the energy and mineral resources sector, the transportation sector, the financial sector, the health sector, the information and communication technology sector, the food sector, the defense sector, and other sectors determined by the President.

This Government Regulation is also emphasized by the issuance of Presidential Regulation Number 82 of 2022 concerning the Protection of Vital Information Infrastructure. In general, there are still similarities in the strategic sector, but there is an explanation regarding other sectors determined by the President as in Article 4 paragraph (2) that the other sectors referred to are strategic sectors where if there is disruption, damage, and/or destruction to IIV in the sector in question, it will have a serious impact on the public interest, public services, defense and security, or the national economy. Together with these implementing regulations, it is hoped that law enforcement can also implement Article 52 paragraph (3) of the ITE Law to realize justice along with the benefits and legal certainty for crackers against government-owned electronic systems based on the cases to be resolved.

According to Mr. Mokhamad Ngajib, Head of the Cyber Crime Unit at Makassar City Police, the enforcement or application of Article 52 paragraph (2) and paragraph (3) of the ITE Law on crackers of government electronic systems has not yet achieved a level of success. The cause is the inconsistency in the application of the aggravating rules to the Public Prosecutor's indictment in concrete cases. In addition, the aggravating rules should be able to be applied subsidiaryly in the Public Prosecutor's indictment, but such an indictment has not yet been obtained. Thus, the rules that have been formed in such a way by providing aggravating criminal penalties become raw and difficult to overcome cracking crimes. The regulation

also fails to achieve its intended purpose of deterring perpetrators and preventing the public from hacking government electronic systems because it has not been fully implemented.

According to Mr. Mokhamad Ngajib, Head of the Cyber Crime Unit at the Makassar City Police, law enforcement requires several interconnected subsystems to achieve order and security, particularly at the legal formulation stage, which emphasizes how to create good laws, the law enforcement stage, and, of course, as a form of legal culture, the level of legal awareness of the community itself. Therefore, it is important to consider proportional balance when examining how law enforcement is implemented. Although in practice, achieving a balance between these components in law enforcement is not easy.

2. Characteristics of Cracking Crime as a Modern Cybercrime.

Cracking is a form of cybercrime with unique characteristics that fundamentally differ from conventional crime. Conceptually, cracking is not limited to breaching security systems, but also encompasses various illegal activities such as data theft, information manipulation, malware insertion, and system disruption. In this context, cracking is a crime that not only attacks technological systems but also undermines public trust in digital security, the foundation of modern society. The main characteristic of this crime lies in its non-physical, anonymous, borderless, and high-tech nature. Unlike conventional crimes that require the perpetrator's physical presence at the scene, cracking can be carried out from any location without geographical boundaries. This blurs legal jurisdiction and often leads to conflicts of authority between countries. Furthermore, the anonymity of the perpetrator, protected by technologies such as Virtual Private Networks (VPNs), encryption, and proxy servers, further complicates the identification and law enforcement process.[7]

From a modern criminological perspective, cracking can be categorized as both a white-collar crime and a cyber-dependent crime. As a white-collar crime, perpetrators generally possess a high level of education and technical expertise, and exploit gaps in technological systems to gain profit. Meanwhile, as a cyber-dependent crime, the existence of information technology is a primary prerequisite for the crime.[13] Therefore, this crime would be impossible without digital infrastructure, demonstrating that technological development is directly proportional to the potential for new crimes. Furthermore, cracking has a broad and multidimensional impact. The losses incurred are not only economic, such as the loss of digital assets or financial losses, but also encompass non-economic aspects such as reputational damage, privacy violations, and disruption to the stability of an institution's information system. In the context of a nation, cracking attacks can even threaten national security if they target strategic systems such as banking, public infrastructure, or government data. Therefore, cracking cannot be viewed as an ordinary crime, but rather as a serious threat to the global digital ecosystem.[14]

Furthermore, another prominent characteristic is the high latency in revealing the crime (time lag in detection), where the crime is often only discovered after the damage has occurred. This is due to the covert nature of the attack and the ever-evolving exploitation techniques. Crackers also tend to use adaptive and dynamic methods, such as phishing, brute-force

attacks, and vulnerability exploitation, which necessitates constant updating of defense systems.

In the context of Islamic law, the phenomenon of cracking can be classified as a form of contemporary crime (al-jarimah al-mu'ashirah) not explicitly mentioned in the texts of the Quran or Hadith. However, through a qiyas (legal analogy) approach, this act shares similarities with several classical forms of crime, such as sariqah (theft) involving the unauthorized taking of property, and tajassus (espionage or invasion of privacy) involving the illegal access to personal information. Thus, cracking can be understood as a violation of the principles of property protection (hifz al-mal) and honor and privacy (hifz al-'irdh). Furthermore, within the framework of Islamic criminal law, cracking falls under the category of ta'zir crimes, namely crimes for which there are no definite sanctions stipulated in the texts, so that the determination of the type and severity of punishment is left to the authorities (ulil amri) based on considerations of public interest. This flexibility is an advantage of Islamic law in responding to the dynamics of modern crime, as it allows for adaptation to new forms of crime that continue to develop along with technological advances.[12]

The ta'zir approach also opens up space for the application of sanctions that are not solely repressive, but also preventative and educational. In the context of cracking, sanctions can include criminal penalties, fines, restitution to victims, and even rehabilitation of perpetrators through digital ethics education. This aligns with the goals of Islamic law, which emphasize not only retributive justice but also reformative justice and preventative justice. The effectiveness of Islamic law enforcement against digital crime (cracking) can be comprehensively analyzed through the maqasid al-shariah approach, namely the primary objectives of Islamic law in safeguarding the five fundamental aspects of human life (al-daruriyyat al-khams), which include the protection of religion (hifz al-din), life (hifz al-nafs), reason (hifz al-'aql), property (hifz al-mal), and honor (hifz al-'irdh). In the context of the crime of cracking, at least two aspects are directly violated: hifz al-mal and hifz al-'irdh.[15] A breach of a digital security system that results in theft or manipulation of data constitutes a form of usurpation of legitimate property rights, while illegal access to personal information represents a violation of individual privacy and dignity. However, upon closer examination, cracking also has the potential to disrupt other aspects of the maqasid al-shariah (Islamic principles), such as hifz al-‘aql (protection of reason) through the dissemination of manipulated or misleading information, and hifz al-nafs (protection of the self) if cyberattacks target vital systems like healthcare or public infrastructure. Therefore, this crime poses a broad and systemic threat, necessitating a legal approach that is not merely partial but addresses the fundamental objectives of sharia as a whole.

Islamic law, in this regard, offers a more comprehensive approach than positive law alone, as it focuses not only on repressive aspects (action after a crime has occurred) but also integrates preventive and educational dimensions. The preventive approach is reflected in the emphasis on prohibiting wrongdoing and the principle of caution (ihtiyat) in social interactions, including in the digital space. Meanwhile, the educational approach is realized through the internalization of moral values such as honesty (sidq), trustworthiness, and responsibility in the use of technology.

Within the framework of Islamic criminal law, cracking is categorized as a ta'zir crime, which provides flexibility to authorities (ulil amri) in determining the type and form of sanctions. This flexibility is particularly relevant in addressing the ever-evolving and highly complex nature of cybercrime. Ta'zir sanctions can be formulated proportionally based on the level of loss, social impact, and the perpetrator's level of culpability, ranging from administrative penalties, fines (gharamah), restitution to victims, restrictions on technology access, to imprisonment. In certain contexts, rehabilitative approaches such as digital ethics training or moral development can even be part of the sentencing strategy. Furthermore, the effectiveness of Islamic law also lies in its moral and spiritual approach, which emphasizes the importance of an individual's internal awareness. Unlike positive law, which tends to be external and coercive, Islamic law seeks to foster self-control (self-regulation) through the concept of taklif (individual responsibility before God). In this context, each individual is viewed as a moral subject responsible for their every action, including in the digital space, which is often considered "value-free." The concept of hisbah as a social oversight mechanism also holds significant relevance in preventing the crime of cracking. Hisbah serves not only as an institutional control but also as a form of community participation in maintaining order and preventing evil. In the digital era, this concept can be actualized through strengthening digital literacy, actively reporting suspicious activity, and building communities aware of the importance of cybersecurity. On the other hand, the effectiveness of Islamic law enforcement in the context of crime-cracking must also be assessed in terms of its ability to create a balance between justice and the public interest (al-'adl wa al-maslahah). Sanctions are not solely intended to punish, but also to restore victims' losses, prevent recurrence of crimes, and maintain social stability. In this regard, a restorative approach based on the principles of Islamic justice has great potential for application, particularly in cases involving non-physical losses such as data theft.

However, the application of Islamic law in the context of a modern state like Indonesia cannot be carried out partially or separately from the prevailing positive legal system. Therefore, an integrative law enforcement model is needed, combining the power of formal regulations with the ethical and moral values of Islamic law. This integration can be achieved through regulatory harmonization, increasing the capacity of law enforcement officials to understand Sharia values, and strengthening ethics-based legal education. Thus, the effectiveness of enforcing Islamic law against cracking as a digital crime does not only lie in the normative or sanction aspects alone, but also in its ability to build a legal system that is holistic, adaptive, and oriented towards substantive justice.

D. CONCLUSION

Cracking is a form of modern cybercrime with specific characteristics: it is non-physical, anonymous, cross-border, and high-tech. This complexity makes cracking a crime that is difficult to detect and handle using conventional legal approaches. From an Islamic legal perspective, cracking can be classified as a digital crime that falls under the category of ta'zir crimes, because although not explicitly regulated in the texts, the act shares a common 'illat' with crimes against property and violations of privacy. Law enforcement against cracking in Makassar City, particularly by the South Sulawesi Regional Police, has a strong legal basis through applicable regulations. However, in practice, the effectiveness of law enforcement still

faces various obstacles, both technically, structurally, and culturally. Limited human resources with digital forensic competencies, minimal technological facilities and infrastructure, and low public legal awareness are the main factors hampering optimal law enforcement against this cybercrime.

E. REFERENCE

[1] A. Handayani, Nurlaelah, S. Hidayat, and D. N. Saputra, "Penegakan Hukum Terhadap Praktik Judi Online di Era Digital: Studi Kasus Cyber crime di Indonesia," *Al-Zayn J. Ilmu Sos. Huk.*, vol. 3, no. 2, pp. 207–215, 2025, doi: 10.61104/alz.v3i2.984.

[2] Januri, D. P. Melati, and Muhadi, "UPAYA KEPOLISIAN DALAM PENANGGULANGAN KEJAHATAN CYBER TERORGANISIR," *Audi AP J. Penelit. Huk.*, vol. 01, no. 02, pp. 94–100, 2022, doi: https://doi.org/10.24967/jaeap.v1i02.1692.

[3] R. A. Hartiwiningsih, *Child Protection from Cyber Violence: An Analysis of CRC General Comment No. 25 and Contemporary Islamic Ethical Perspectives in Indonesia and Malaysia*, vol. 5, no. 1. 2026.

[4] E. Y. Purwanti, "Implementation of Environmental Education Value in Islamic Education (Analysis of Tafsir Al Qur'an Surah Al-A'raf Ayat 56-58)," *Lisyabab J. Stud. Islam dan Sos.*, vol. 2, no. 2, pp. 161–172, 2021, doi: 10.58326/jurnallisyabab.v2i2.87.

[5] M. Asas Peradilan Yang Cepat, D. Biaya Ringan Zulqisthi Hasbi Kawu, A. Razak, M. Ya, and rif Arifin, "Eksistensi Pemeriksaan Perkara Secara Elektronik (E-Court) Dalam," *J. Lex Philos.*, vol. 4, no. 2, p. 2023.

[6] J. Riset and M. Edukasi, "Dampak teknologi ai terhadap pola kejahatan," vol. 3, pp. 304–316, 2026.

[7] A. Angkutan, U. Risman, H. Mustafa, M. Pawennai, and M. Mursyid, "Peretasan Terhadap Sistem Elektronik Pada," 2020.

[8] Y. Ansari and D. Sukarja, "Legal Aspects of Cross-Border Electronic Commerce Transactions with Quick Response Code (QR Code) Based Payments in the ASEAN Cooperation Framework," vol. 4, no. 6, pp. 2419–2429, 2024.

[9] M. R. Kurniarullah, T. Nabila, A. Khalidy, V. J. Tan, and H. Widiyani, "Tinjauan Kriminologi Terhadap Penyalahgunaan Artificial Intelligence: Deepfake Pornografi dan Pencurian Data Pribadi," vol. 10, no. 10, pp. 534–547, 2024.

[10] M. M. F. ramadhan. Andi Muhammad Fikri, "Law Enforcement in Child Fighting Crimes That Result in Death," *J. Huk. HorizonPublicLegal Stud.*, vol. 4, no. 1, pp. 1–30, Feb.

2024, doi: 10.15294/panjar.v4i1.55017.

[11] A. J. Politik, H. Humaniora, V. Nomor, H. S. Quratuainniza, and E. Nurkhaerani, "Regulasi Kecerdasan Buatan untuk Mengatasi Penyalahgunaan Deepfake di Indonesia Fakultas Hukum , Universitas pembangunan Nasional ' Veteran ' Jakarta melakukan Tindakan kejahatan maupun sebagai objek dari kejahatan tersebut .," vol. 4.

[12] D. U. Informasi *et al.*, "KEBIJAKAN FORMULASI TINDAK PIDANA DEEPFAKE ELEKTRONIK (UU ITE) DAN UNDANG-UNDANG," vol. 12, no. 1, pp. 157–169, 2026, doi: 10.55809/tora.v12i1.647.

[13] P. D. Humaniora *et al.*, "Enforcement of the ITE Law and the Impact of Online Gambling Promotion by Influencers on the Youth in Tomohon," vol. 8, no. 2, pp. 2268–2279, 2024, doi: 10.36526/js.v3i2.

[14] M. S. R. Ventry Faomassi zega, Hernita Aruan, Roni Dear A Purba, "Pertanggungjawabaan Pidana Selebgram Dalam mempromosikan Judi Menurut UU ITE," vol. 5, no. 3, pp. 494–504, 2021, doi: 10.36312/jisip.v5i3.2194.

[15] N. A. Adlina, "Efektivitas Penegakan Hukum Perjudian Online di Indonesia: Mengatasi Hambatan Regulasi dan Implementasi," *J. Contemp. Law Stud.*, vol. 2, no. 2, pp. 197–208, 2025, doi: 10.47134/lawstudies.v2i2.3670.